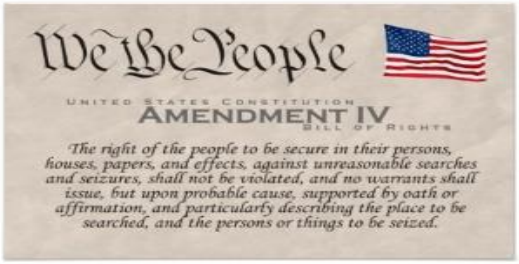
Cell Phones: What They May Contain, How to Get It and How to Get It Admitted

UPC Fall Conference
September 12, 2013

Kristine Knowlton, ICAC Prosecution Section Chief
Utah Attorney General's Office

Copyright Info

- This multimedia presentation contains the creative work of others and is used by permission, because of public domain, or under a claim of the fair use pursuant to 17 USC 107. Further distribution or use is not permitted without authorization
- Credit also to:
  - Homeland Security Federal law Enforcement Training Centers
  - Law Clerk extraordinaire: Jessica Malmquist



Legal Issues in Searching Cell Phone and Other Electronic Devices

- Basic Premise: citizens have reasonable expectation of privacy in home, person and property
- Government access requires: warrant; consent; or exception to warrant

Cell phones and other similar devices are the tools of the modern criminal

- Can be used to store evidence of a crime
- Can be used as instrumentality of crime: plan; commit; even record commission of crime
- Been described as "virtual biographers of our daily activities"

What does prosecutor do

- When you want to know what the device contains?
- When you want to know where a cell phone has been?
- When you want to know who the subscriber of the service is?
- When you want to know the contents of the communications?

WHEN YOU WANT TO KNOW WHAT THE DEVICE CONTAINS

- Search Warrant
- Consent
- Exceptions to Warrant
  - Exigent circumstances
    - Prevent destruction of evidence
    - Public safety and safety of officer
  - Mobile Conveyance
  - Inventory
  - Search Incident to Arrest (SIA)
  - Inevitable Discovery

Search Warrant

- When there's time to do so, should always get a warrant
- Special considerations
  - You want to search for and obtain DATA that is evidence of a crime
    - Images, contact lists, text messages, emails, videos, calendars, appointments, apps, websites, search terms, accounts, user names, etc.
    - When you focus on the data you want, then you can request warrant for authorization to search anywhere that data might be found, including cell phone, computers, etc.

- Is the device an instrumentality of the crime?
- Probable cause considerations
  - Calls to or from target to witness or CI
  - Texts
  - Call logs
  - Articulate knowledge that cell phones often used in commission of crimes: used by lookouts; used to arrange meeting times and places for customers
  - Articulate knowledge that suspects may take photos to plan their crimes…photos of security and surveillance cameras, guard posts
  - Articulate knowledge that not unusual for suspects to take photos of victims, send anonymous or fake user named texts or emails, use "throw away phones" in stalking and harassment cases
  - Articulate knowledge that it's not unusual for suspects to takes videos or pictures of themselves committing the crime

Consent

- May be limited in scope
  - Consent to look at phone logs and officer sees child porn; officer seizes phone as evidence of a crime and applies for SW
- May be revoked
  - If officer has already recognized evidence of a crime on a phone and suspect revokes consent, officer can still seize phone to prevent destruction of data under exigent circumstances…then decide if can search or apply for warrant

Exceptions to Warrant

- **Exigent circumstances**
  - Officer has PC there is evidence of a crime and that evidence might be immediately destroyed, it is reasonable to seize the evidence or the container it's in to **prevent its destruction**
    - If search of evidence or container also necessary to prevent its destruction, then search permissible
      - Must be able to articulate knowledge that data can be remotely deleted or altered and that phone was lawfully seized
      - ***US v Wurie*** 1st Circuit No 11-1792, 5/17/2013..officer seized phone from suspect's person as SIA and then searched phone's data w/o warrant. Court held search exceeded SIA exception and noted that the govt didn't argue justification under exigent circumstances (such as necessity to prevent immediate destruction) or any other exception.**** August, 2013**...Govt filed petition for S Ct to hear and rev 1st Circuit decision
      - See also ***US v Mercado-Nava***, 486 F Supp 2d 1271 (D.Kan. 2007)

- **Public safety and safety of officer**
  - ***US v Lottie***, 2008 WL 150046 (unpublished)
    - Counter-surveillance caused concern for officer safety and for the public in the midst of a large drug transaction and entitled officers to immediately search cell phone

Exception to warrant cont.

- **Mobile Conveyance**
  - If a car is readily mobile and PC exists to believe it contains contraband or evidence of the commission of a crime, the 4th Amendment permits the police to search vehicle as well as containers in the vehicle (***Carroll v US*** 267 US 132 (1925), ***Pennsylvania v Labron*** 518 US 938 (1996)
  - Electronic communication device considered "container" by some courts, other courts have compared it to a file cabinet; best practice is to get a SW

- ***US v Rocha***, 2008 WL 4498950
  - officers searched vehicle after traffic stop and found drugs and 4 cell phones. Detective recovered contact lists, numbers dialed and recent calls from each phone w/o search warrant
  - Court held that because PC existed to believe evidence of a crime would be found in cell phone information, the automobile exception allows the search of the cell phone just as any other container

"The Drug Baron is not well today. He has had a seizure."

Warrant exception cont.

- **Inventory**
  - LE agency must have standard inventory policy specifically addressing search of electronic devices in order to justify searching cell phones
  - **CAVEAT**: even if agency has policy re: data searches, it probably would be unconstitutional as purpose of inventory is TO PROTECT property taken by the govt
  - Could also put data at risk of destruction by turning on device to inventory data

- See ***US v Wall***, 2008 US Dist. LEXIS 103058, 10 (S.D. Fla 2008)
  - Court recognized cell phone may be identified as item seized during post arrest inventory, "However, there is no need to document the phone numbers, photos, text messages or other data stored in the memory of a cell phone to properly inventory the person's possessions because the threat of theft concerns the cell phone itself, not the electronic information stored on it."

- **Search Incident to Arrest - SIA**
  - ***US v Finley***, 477 F3d 250 (5th Cir 2007)
    - Leading example of permissible cell phone search incident to arrest, analogizing cell phone to closed container
      - Other courts decline that analogy stating that the quantity and quality of info contained in electronic device distinguishes it from other physical containers…see ***US v Park***, 2007 WL 1521573 (unpublished) and mentioned by a federal court in Tenth Cir in ***US v Gutierrez***, 2008 WL 2397668
      - Court may differentiate between cell phone found on person and cell phone found in immediate
      - Consider exigent circumstances necessitating search

- ***Silvan v Briggs***, 2009 US App. LEXIS 1520 (10th Cir 2009, unpublished but facts available at 2009 WL 159429)
  - Civil rights lawsuit where claimants argued warrantless search of cell phone incident to arrest as 4th Am violation. 10th Cir held search lawful and dismissed lawsuit.

- Officer must be able to articulate evidence in cell phone destructible thus necessitating immediate search
  - Cell phones almost always have finite memory which impacts size of call log as well as # of text messages it can hold; new calls or texts could replace older calls and texts, thereby bumping the older data from the phone before SW can be obtained
  - Owner can arrange for remote access by another person to delete data, even when phone in hands of police

- Best case is for officer to articulate both an SIA and an exigent circumstance to justify search of cell phone for data
  - **REMEMBER**: must have PC that evidence on phone to support exigent circumstance exception, which is not necessary in SIA; and SIA must also be substantially contemporaneous to arrest
- See ***US v Parada***, 289 F Supp 2d 1291 (D. Kan. 2003)
  - SIA and inventory search and exigency to prevent destruction of evidence

- **Inevitable Discovery**
  - US v Morales-Ortiz, 376 F Supp 2d 1131 (D. N.M. 2004)
    - DEA agents executed arrest warrant for defendant at his residence. While conducting protective sweep, they found a pager and searched through the messages on it as well as searched through numbers found in a cell phone. Court held that even though the items were originally unlawfully searched, the contents were still admissible under inevitable discovery as the pager and cell phone would have been searched legally pursuant to search warrant

WHEN YOU WANT TO KNOW WHERE CELL PHONE HAS BEEN

- **Emergency circumstances** (i.e. kidnapping, etc.)
  - Exigent circumstance exception
  - Emergency Aid Doctrine or Community Caretaker exception
    - Police must have reasonable grounds to believe emergency exists
    - Entry into home/car must be reasonable attempt to protect life, safety
    - Scope of search must be related to protection, preservation of life
      - See ***Brigham City v Stuart***, US SCt 2006
    - See also 18USC §2702, reasonable belief of immediate danger of death or serious bodily injury, provider may disclose records to govt

- **Business records exception**
  - In ***Re: Application of the USA for Historical Cell Site Data***, 11-20884, 7/30/2013, 5th Cir
    - Warrantless search for historical data directly from communications carrier constitutional as location was "clearly a business record" and not protected by 4th Am but governed by federal Stored Communications Act SCA (18 USC§ 2793
    - Govt has right to warrantless searches for business records which are created by phone companies (third party doctrine) for billing customers for phone use. The SCA requires specific and articulable facts by LE to obtain order for that data which enables judicial branch to prevent and remedy over reaching
    - Cases in two other circuits are pending

- **Get search warrant otherwise**
  - Cell tower pings
  - Call origination
  - Call termination
  - Victim phone/suspect phone

WHEN YOU WANT TO KNOW WHO THE SUBSCRIBER OF THE SERVICE IS

- **State administrative subpoena** §77-22-2.5
  - Can only be used for investigations involving sexual offense against child, stalking and child kidnapping
  - Can only obtain subscriber info, NOT CONTENT
    - Names, addresses, local and long distance telephone connections, records of session times and duration, length of service, including start date and types of services utilized, telephone or other instrument subscriber numbers or identifiers, including temporarily assigned network addresses

- State statute based on federal Stored Communications Act
- Statute specifies non-disclosure by provider to subscriber §77-22-2.5(5)
- Govt not required to provide notice to subscriber §77-23b-4(3)(b)

- **Search warrant for third party service provider**
  - Rule 40(c)(2) URCrP
    - If no cause to believe 3rd party involved in criminal behavior, **no search warrant shall issue except on finding by magistrate that evidence sought to be seized cannot be obtained by subpoena or that such evidence would be concealed, destroyed, damaged or altered if sought by subpoena**.
    - Notification to subscriber required, though may be delayed. §77-23b-6(1)(e)

WHEN YOU WANT TO KNOW CONTENTS OF COMMUNICATIONS

- **GET A SEARCH WARRANT**
  - Still subject to federal and state Stored Communications Acts
  - Can request delay of notification by provider to subscriber and by govt to subscriber §77-23b-(6)(1)(a)
    - Not to exceed 90 days; may get extension up to add'l 90 days
    - Requires written certification of supervisory official that there is reason to believe notification of existence of warrant may have adverse result

- Delay in notification by govt to subscriber
  - Notice provision - §77-23b-(6)(1)(e) requires govt to provide to subscriber
    - Copy of warrant/process
    - Plus notification/certification letter

IMPORTANT

- Read both when dealing with electronic communications
  - Title 77, Chapter 23b
  - Title 77, Chapter 22, Section 2.5

The Electronic Frontier Foundation www.eff.org